



PDSD NEWS

Personnel & Document Security Division
Office of Homeland Security & Emergency Coordination
Departmental Management

A Note from the Chief...

As Fiscal Year 2010 comes to a close, we begin to closely focus on the challenges facing USDA's personnel and information security programs in the upcoming fiscal year.

We continue our efforts to modernize personnel security processes, which include the implementation of OPM's eDelivery system, enabling a headquarters LiveScan fingerprint connection to the Department of Justice, and the imaging of existing hard copy personnel security files.

Our Information Security Staff will strive to update an existing online security refresher briefing in Aglearn and explore the possibility of providing automated Sensitive Compartmented Information refresher briefings, plus directly assist agencies in improving ways to safeguard classified national security information.

While our personnel security programs face significant challenges to integrate new Public Trust and Continuous Evaluation reinvestigation programs in the midst of shrinking budgets, the PSDS staff looks forward to working with USDA agencies to find reasonable solutions to these and other difficult problems.

Susan Gulbranson, Chief of PSDS

UPCOMING EVENTS

10/1/10 – LIVE NOW

Updated Position Designation Automated Tool

OPM released an updated version of the Position Designation Automated Tool in the Secure Portal to match the FY11 aligned investigation products.

10/6/10 & 10/20/10

11/3/10 & 11/17/10

Security Briefing – By Reservation Only

Indoctrination briefing for new security clearance holders by the InfoSec staff in the South Building, RM S-310, 11am.

11/30/10-12/1/10

Annual Security Professionals Seminar

OPM will host the annual seminar at the Sheraton Premiere at Tysons Corner. The cost for the two-day seminar is \$150. The final registration deadline is Friday, November 5, 2010.

12/30/10

e-QIP Validation Enhancements

OPM is enhancing data validation in e-QIP to reduce unacceptable investigation requests. Some free text fields will change to drop-down boxes. Saved data in e-QIP will now require the applicant to reenter that data in the new format on subsequent submissions.

NEWSWORTHY

IN THIS ISSUE

PAGE 3 FY11 INVESTIGATIONS MENU

Check out the changes
beginning Oct 1st

PAGE 3 COMING SOON

Future developments
underway at OPM

PAGE 4 LEADER OF THE PACK

Congrats to a stand out
Agency POC

PAGE 4 INTERNAL NETWORK VULNERABILITIES

Top 10 list

PAGE 5 REVISED AD-1187

For immediate use

PAGE 5 NEED HELP?

Who to contact in PDSD
for assistance

PAGE 5 SECURITY PACKAGE REMINDERS

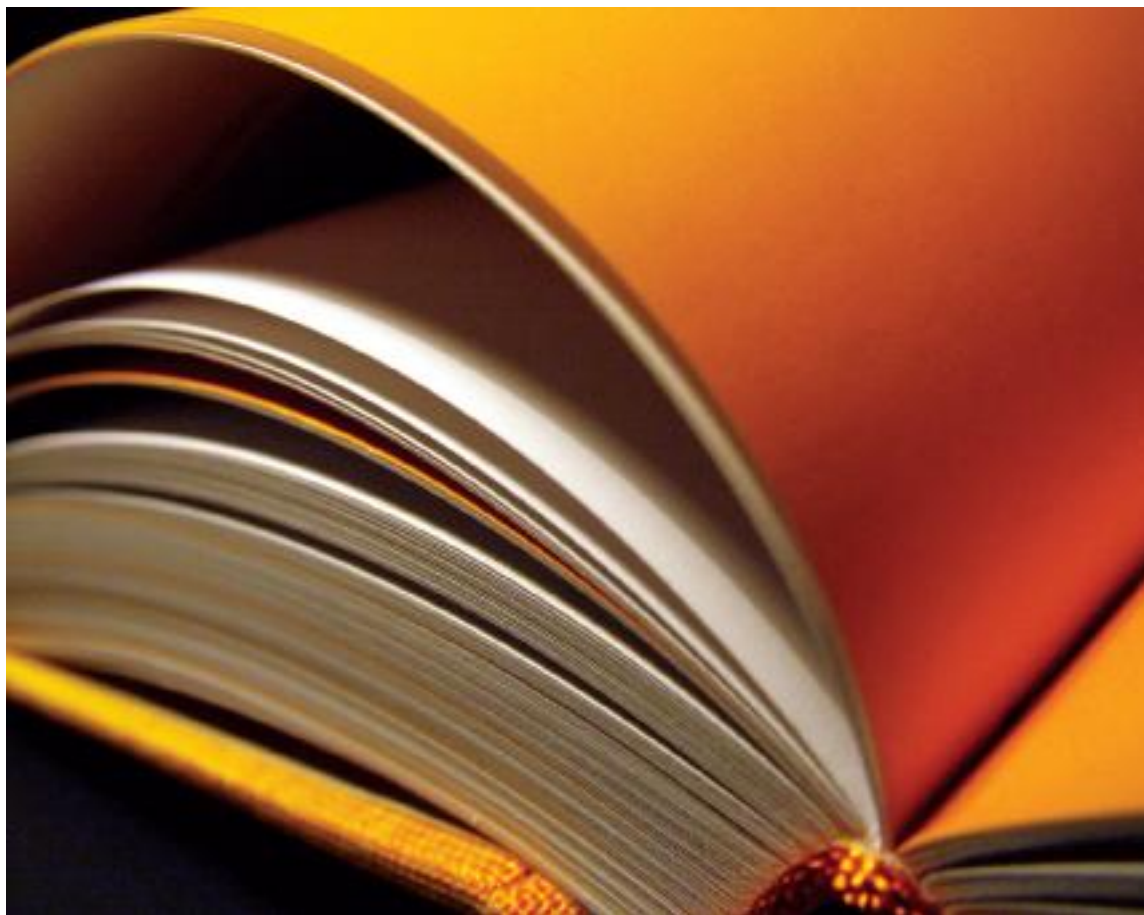
Reminders to address
common errors

USDA/DM/OHSEC/PDSD
1400 Independence Ave,
SW, RM S-310
Washington, DC
20250-5050

(202) 720-7373 – main
(202) 720-1689 – fax

pdsd@dm.usda.gov

[PDSD Website](#)



READ ALL ABOUT IT...

H.R. 3149, EQUAL EMPLOYMENT FOR ALL ACT, LIMITING THE USE OF CREDIT REPORTS, REP STEVE COHEN, INTRODUCED JULY 2010:

<http://www.govtrack.us/congress/bill.xpd?bill=h111-3149>

FORMER WORKERS AT LOS ALAMOS CHARGED WITH TRANSMITTING CLASSIFIED NUCLEAR WEAPONS DATA TO INJURE THE UNITED STATES, DOJ, SEPT 2010:

<http://www.justice.gov/opa/pr/2010/September/10-nsd-1044.html>

DEBT AND HOME FORECLOSURES: THEIR EFFECT ON NATIONAL SECURITY CLEARANCES, SHELDON COHEN, SEPT 2010:

<http://www.sheldoncohen.com/publications/Article%20on%20Guideline%20F.pdf>

S.3790, PERSONS HAVING SERIOUSLY DELINQUENT TAX DEBTS SHOULD BE INELIGIBLE FOR FEDERAL EMPLOYMENT, SEN TOM COBURN, INTRODUCED SEPT 2010:

http://coburn.senate.gov/public//index.cfm?a=Files.Serve&File_id=7fa88f75-6fb6-4764-bae4-b291c5fba112

FY11 Investigations Menu

PUBLIC TRUST POSITIONS

MBI-15 \$809 (CODE A) \$752 (CODE C)

The MBI is the initial investigation for Moderate Risk positions. Use the SF85P, Questionnaire for Public Trust Positions, to request this investigation. Case service code A does not relate to case completion time, rather it refers to expedited law record searches.

NACLC-08 \$228 (CODE B)

The NACLC is the proposed reinvestigation type for Moderate Risk Public Trust positions. Use the SF85P to request this investigation.

BI-25 \$3,780 (CODE A) \$3,189 (CODE C)

The BI is the initial investigation for High Risk positions. Use the SF85P to request this investigation.

PRI-11 \$715 (CODE A) \$630 (CODE C)

The PRI is the proposed reinvestigation type for High Risk Public Trust positions. Use the SF85P to request this investigation.

NATIONAL SECURITY POSITIONS

ANACI-09 \$260 (CODE B)

The ANACI is the initial investigation for Non-Critical Sensitive positions at the Confidential or Secret level. Use the SF86, Questionnaire for National Security Positions, to request this investigation.

NACLC-08 \$228 (CODE B)

The NACLC is the reinvestigation type for Non-Critical Sensitive positions at the Confidential or Secret level. Use the SF86 to request this investigation.

SSBI-30 \$4,399 (CODE A) \$4,005 (CODE C)

The SSBI is the initial investigation for Critical Sensitive or Special Sensitive positions at the Top Secret or TS/SCI level. Use the SF86 to request this investigation.

SSBI-PR-18 \$2,964 (CODE A) \$2,711 (CODE C)

The SSBI-PR is the reinvestigation type for Critical Sensitive or Special Sensitive positions at the Top Secret or TS/SCI level IF there ARE self-disclosed security concerns on the questionnaire. Use the SF86 to request this investigation.

PPR-19 \$2,261 (CODE A) \$2,009 (CODE C)

The PPR is the reinvestigation type for Critical Sensitive or Special Sensitive positions at the Top Secret or TS/SCI level IF there ARE NO self-disclosed security concerns on the questionnaire. Use the SF86 to request this investigation.

HIGHLIGHTS

Eliminated Investigations

LBI

PRIR

PTSBI

BGI

SGI

Reciprocity

There will be no negative effect on reciprocity. All old investigations will stand. For example, we can accept a previously completed LBI for a Moderate Risk position.

COMING SOON

Implement revised SF-86 (e-QIP) with expanded (branching) questions and revised consent forms (Responsible entity: OPM) *December 2010*

Continue Security and Suitability oversight visits and audit programs to review agency position designation alignment and monitor compliance (Responsible entities: ODNI/OPM) *December 2010*

Develop Suitability and Security adjudicator training (Responsible entities: DoD/OPM) *December 2010*

Submit next version of SF-85P to Federal Register for public comment (Responsible entity: OPM) *December 2010*

LEADER OF THE PACK

In each quarterly newsletter, PDSD is going to give a shout out to one of our agency points-of-contact who has been going above and beyond in providing excellent personnel security assistance to PDSD.

This issue, we would like to thank Dru Dukart with APHIS! Dru handles an agency that has one of the highest numbers of investigation requests. She is thorough, inquisitive, receptive, and a delight to work with. Keep up the great work Dru!



TOP 10 LIST OF INTERNAL NETWORK VULNERABILITIES

The Information Security Staff has seen a rise in articles relating to concerns from government technology agencies over the past several months on the cyber threats that exist to exploit information. In September, Government Technology came out with an article that puts these concerns in perspective. On September 20th, a staff writer for GovTech, Hilton Collins, penned an article "Top 10 Network Security Threats." He writes regarding the daily cyber-threats that each agency must combat and some helpful advice on what to look for. Derek Manky, who is a project manager for cyber security and threat research from Fortinet adds, "The ways that the networks can be compromised five years ago internally, can still exist. It's just that today, that list is really growing, and that's why this is ongoing research."

According to Manky and other researchers that deal with these threats on a daily basis, the "Top-10" list of internal network vulnerabilities are:

- USB Drives
- Laptops and netbooks
- Wireless access points
- Miscellaneous USB devices (digital cameras, MP3 players, etc.)
- Employees borrowing others' machines or devices

- The Trojan Human (attackers who visit sites disguised as employee or contractors)
- Optical media (CDs, DVDs, etc.)
- Lack of employee alertness
- Smartphones
- E-mail

All of the listed items are concerns that can lead to potential information security breaches here at USDA. PDSD along with the Office of the Chief Information Officer's office instructs employees to remain vigilant with the use of computers, the transfer of information and the introduction of any outside software or hardware into the systems we use. None of our employees should bring in personal USB drives or other electronic devices that have been used outside the agency. These can have viruses on them that can potentially put our cyber infrastructure at risk. Both offices are also concerned about the transfer of work related information to and from home computers from your office system due to the potential for data to be corrupted or compromised. Please take the opportunity to review DM 3440-2 Control and Protection of Sensitive Security Information.

Both offices also promote the use of Autoberry to protect our traveling staff members to guard their Blackberrys from potential intrusion. You can contact the service desk at DM.ServiceDesk@usda.gov or call them at (202) 720-1716.

TOOLS: Secure Portal and CVS

OPM's Secure Portal is a gateway to OPM products and services. Membership in this Portal is by invitation only, limited to those having official business with us, and others in the personnel security community. The portal includes a library of reference material and links to the Central Verification System (CVS) for reciprocity handling. To request access, email Opal Jones at opal.jones@dm.usda.gov.

If you have forgotten your username and or password to access the Secure Portal, please contact their Help Desk at (877) 624-3771 or email: helpdesk@nc4.us. The Help Desk is available Monday through Friday from 8:00am to 8:00pm EST.

REVISED AD-1187 FORM

PDSD Bulletin #11-01 announced the latest version of the AD-1187, Request for Personnel Security Services form. Agencies must begin to use this new version starting October 1, 2010. Please discard of all previous hardcopy and electronic versions as prior versions will not be accepted.

The revised form includes updates to the "Type of Investigation" section to match with the aligned investigative products offered by OPM for FY11.

Agency POC's are reminded that the AD-1187 must be fully and accurately completed in order for PDSD to process the request. This includes selecting the correct action you want PDSD to take in the first section, marking the proper position designation, providing an email address (especially for contractor employees), and ensuring that an authorized person has signed the request.

If you have any questions about the AD-1187 or selecting the proper level of investigation, please contact PDSD at (202) 720-7373. Please refer to PDSD Bulletin #10-09 for information on the aligned OPM investigations for FY11 at <http://www.dm.usda.gov/pdsd/bulletins.htm>.

HOW CAN WE HELP YOU?

POLICY

For policy and guidance assistance, contact John Loveless at john.loveless@dm.usda.gov or (202) 720-0540.

WEBSSETS GUIDANCE

For assistance on using webSETS, contact Carrie Moore at carrie.moore@dm.usda.gov or (202) 720-3487.

PASS A CLEARANCE

To check on requests to pass a clearance, please contact Kelly Panganiban at kelly.panganiban@dm.usda.gov or (202) 720-7373.

e-QIP and CVS ACCESS

For e-QIP and CVS access, contact Opal Jones at opal.jones@dm.usda.gov or (202) 720-0017.

FORMS PROCESSING

For questions regarding e-QIP submissions and form corrections, contact Lucy Lew at lucy.lew@dm.usda.gov or (202) 720-9388.

WEBSSETS USER ACCESS

To obtain access to webSETS, contact Stephen Milinovich at stephen.milinovich@dm.usda.gov or (202) 720-5155.

SECURITY PACKAGE / e-QIP REMINDERS

- Ensure that the correct version of the AD-1187 (updated Oct 2010) is used.
- On the AD-1187 only one position designation should be checked (a position is either one of National Security or Public Trust and boxes should not be checked in both areas).
- Please be sure to check the investigation type and whether a priority or standard investigation is requested.
- Be sure to include the email address, especially for contract employees.
- We have had a lot discrepancy between the Agency Use Block of eQIP and the AD-1187 form. Please ensure investigation type and position sensitivity levels chosen are consistent.
- Agency Use Block: Be sure to list AG00 as both the SON and the SOI to ensure PDSD receives the closed investigation from OPM.
- Please ensure the security form is reviewed carefully prior to submitting the forms to PDSD. Ensure that all fields are properly completed.
- Ensure all attachments are included in the eQIP submission and are properly attached electronically. Please note that the Fair Credit Release does not need to be scanned; however, it must be included with the AD-1187. If SCI access is being requested, please ensure that the SCI Credit Release is included in the security package.